UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on August 1, 2024

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**UNDER SEAL**
	:	
ERIC COUNCIL JR.,	:	**VIOLATIONS:**
Also known as "Ronin,"	:	
Also known as "AGiantSchnauzer,"	:	**COUNT 1:**
Also known as "@Easymunny,"	:	**18 U.S.C. § 371; 18 U.S.C. § 1028A(a)(1)**
	:	**and 18 U.S.C. § 1029(a)(1) (Conspiracy to**
Defendant.	:	**Commit Aggravated Identity Theft and**
	:	**Access Device Fraud);**
	:	
	:	**FORFEITURE:**
	:	**18 U.S.C. § 981; 21 U.S.C. § 853(p); and 28 U.S.C. § 2461(c)**

INDICTMENT

The Grand Jury charges that, at all times material to this Indictment, on or about the dates and times stated below:

Introduction

1. In late 2023 and early January 2024, the U.S. Securities and Exchange Commission ("SEC") was deliberating over the approval or denial of Bitcoin ("BTC") Exchange Traded Funds ("ETFs"). The SEC's impending decision had been anticipated by market participants for months and had the potential to impact the price of Bitcoin.

2. On January 9, 2024, an unauthorized actor took control of the @SECGov X account (sometimes called the SEC's Twitter account) and transmitted a fake post in the name of the SEC Chairman, falsely announcing, in part, "Today the SEC grants approval for #Bitcoin ETFs for listing on all registered national securities exchanges." This post was transmitted and received

throughout the United States and inside the District of Columbia. Immediately following dissemination of the tweet, the price of BTC increased by more than $1,000 per bitcoin.

3. Shortly after this unauthorized post, the SEC regained control over their X account and confirmed that the announcement was unauthorized and the result of a security breach. Following this corrective disclosure, the value of BTC decreased by more than $2,000 per bitcoin.

4. The SEC and X were able to confirm that an unauthorized actor gained control of the SEC X account through a "SIM swap."

Background Regarding SIM Swapping

5. A Subscriber Identity Module ("SIM") card is a chip that stores information identifying and authenticating a cell phone subscriber. When a cell phone carrier reassigns a phone number from one physical phone to another — such as when a customer purchases a new phone but wants to retain the same number — the carrier switches the assignment of the cell phone number from the SIM card in the old phone to the SIM card in the new phone, a process sometimes referred to as "porting" a number.

6. A SIM swap attack refers to the process of fraudulently inducing a carrier to reassign a cell phone number from the legitimate subscriber or user's SIM card to a SIM card controlled by a criminal actor. SIM swap attacks are often conducted for the purpose of defeating multifactor authentication ("MFA") and/or two-step verification. MFA and two-step verification add an additional layer of security to the authentication process for accessing online accounts, such as financial or social media accounts. A SIM swap attack allows a criminal actor to defeat the MFA and/or two-step verification process to access a victim's account so that the criminal actor may steal money and/or data from the victim.

The Conspiracy

7. During at least in and around January 2024, **ERIC COUNCIL JR.** ("**COUNCIL**"), a resident of Athens, Alabama, conspired with others to carry out a fraudulent SIM swap attack. As part of this scheme, the co-conspirators shared with **COUNCIL** the personal identifying information ("PII") of the intended victim; created a fraudulent identification document in the victim's name; used the fraudulent identification document to impersonate the victim; took over the victim's cellular telephone account; and accessed the online social media accounts linked to the victim's phone line for the purpose of generating fraudulent posts in the name of the SEC Chairman.

Co-Conspirators

8. The co-conspirators in this scheme included the defendant listed below, and others:

a. **COUNCIL** was a member of the conspiracy and used the online monikers "Ronin," "AGiantSchnauzer," and "@Easymunny."

Purpose of the Conspiracy

9. The object of the conspiracy was for **COUNCIL** and others (collectively, the "co-conspirators") to unjustly enrich themselves by targeting victims for SIM swaps, creating fraudulent identification documents in victim names, performing SIM swaps in exchange for money, accessing victims' social media accounts, and concealing the sources and methods of payments for SIM swap services through virtual currency laundering techniques.

Manner and Means

10. In or around January 2024, **COUNCIL** and other co-conspirators, within the District of Columbia and elsewhere, carried out the conspiracy through the following manner and means, among others:

a. **COUNCIL** received victim PII from other co-conspirators by way of SMS and encrypted messaging services;

b. **COUNCIL** received an identification card template containing a victim's name with his face from his co-conspirators by way of SMS and encrypted messaging services;

c. **COUNCIL** used his identification card printer to print a fraudulent identification card;

d. **COUNCIL** traveled to a mobile phone provider store and other retail store to conduct a SIM swap using the fraudulent identification card;

e. **COUNCIL** presented a fraudulent identification card in a victim's name at a mobile phone provider store in order to obtain a SIM card linked to the victim's account;

f. Co-conspirators, after gaining access to the victim's SIM card and phone number, generated, received, and shared with other co-conspirators access device codes to gain unauthorized access to a social media account linked to the victim's phone number; and

g. Co-conspirators used this unauthorized access to change social media account settings and transmit a fraudulent post in the name of the SEC Chairman.

Acts in Furtherance of the Conspiracy

11. In or around January 2024, within the District of Columbia and elsewhere, **COUNCIL**, and others, transferred and used without lawful authority, a victim's means of identification for the purpose of causing the victim's cellular telephone accounts to be transferred

to a phone in his possession.

12. **COUNCIL**, and others, executed a SIM swap of the cellular telephone account associated with victim C.L., among others, in order to obtain things of value.

a. On or about January 9, 2024, a co-conspirator identified victim C.L. as having authorized access over the telephone number linked to the SECGov X account.

b. On or about January 9, 2024, **COUNCIL** received instruction from a co-conspirator to perform a SIM swap of victim C.L.'s cellular telephone account, which was maintained by AT&T.

c. On or about January 9, 2024, **COUNCIL** traveled to an AT&T store in Huntsville, Alabama and presented an identification card in C.L.'s name. **COUNCIL** claimed to be an FBI employee who broke his phone and needed a new SIM card, and thereby obtained a new SIM card tied to C.L.'s account (the "C.L. SIM card").

d. On or about January 9, 2024, after obtaining the C.L. SIM card, **COUNCIL** walked to a Huntsville Apple store and purchased a new iPhone for the purpose of effectuating the SIM swap. **COUNCIL** then inserted the C.L. SIM card into this iPhone in order to receive two-factor security reset codes associated with the @SECGov X account.

e. On or about January 9, 2024, **COUNCIL** received the "X confirmation code" to reset the @SECGov X account and promptly transmitted this code to a co-conspirator.

f. On or about January 9, 2024, a co-conspirator used this fraudulently

obtained security code to gain access to the @SECGov X account.

g. On or about January 9, 2024, a co-conspirator, using such access, issued a fraudulent tweet on the @SECGov X account in the name of the SEC Chairman, falsely announcing the approval by the SEC of BTC ETFs.

h. On or about January 9, 2024, after receiving the reset codes, **COUNCIL** drove to Birmingham, Alabama to return the iPhone for cash.

13. In addition, during and in furtherance of the conspiracy, **COUNCIL** did the following:

a. **COUNCIL** owned, possessed, used, and traveled with an identification card printer used for printing fraudulent identification cards for SIM swaps.

b. **COUNCIL** destroyed fraudulent identification cards after using the cards for SIM swaps.

c. **COUNCIL** received payment for SIM swaps through BTC and other virtual currencies.

d. **COUNCIL** used his personal computer to execute internet searches for the following information and terms among others;

i. "SECGOV hack," "telegram sim swap," "how can I know for sure if I am being investigated by the FBI," "What are the signs that you are under investigation by law enforcement or the FBI even if you have not been contacted by them," "what are some signs that the FBI is after you," "Verizon store list," "federal identity theft statute," and "how long does it take to delete telegram account."

COUNT ONE
(18 U.S.C. §§ 371, 1028A(a)(1), and 1029(a)(1))
(Conspiracy to Commit Aggravated Identity Theft and Access Device Fraud)

14. Paragraphs 1 through 13 are re-alleged herein.

15. In or around January 2024, within the District of Columbia and elsewhere, the defendant,

ERIC COUNCIL JR.,

did knowingly and willfully conspire and agree, with others, to commit offenses against the United States, that is, (a) knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to an enumerated felony violation as defined by Title 18, United States Code, Section 1028A(c), that is Access Device Fraud, in violation of Title 18, United States Code, Section 1028A(a)(1) (Aggravated Identity Theft) and (b) knowingly, and with intent to defraud, produce, use, or traffic in one or more counterfeit access devices, in violation of Title 18, United States Code, Section 1029(a)(1) (Access Device Fraud).

16. In furtherance of the conspiracy and to effect the objects of the conspiracy, the overt acts described above in Paragraphs 11 through 13, among others, were committed in the District of Columbia and elsewhere.

(In violation of Title 18, United States Code, Sections 371, 1028A(a)(1) and 1029(a)(1))

FORFEITURE ALLEGATION

1. Upon conviction of the offense alleged in Count One of this Indictment, the defendant shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to this offense, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

2. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to Title 21, United States Code, Section 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code, Section 2461(c), and Title 21, United States Code, Section 853(p)).

A TRUE BILL

FOREPERSON

Matthew M. Graves/jfh

MATTHEW M. GRAVES
ATTORNEY FOR THE UNITED STATES
IN AND FOR THE DISTRICT OF COLUMBIA